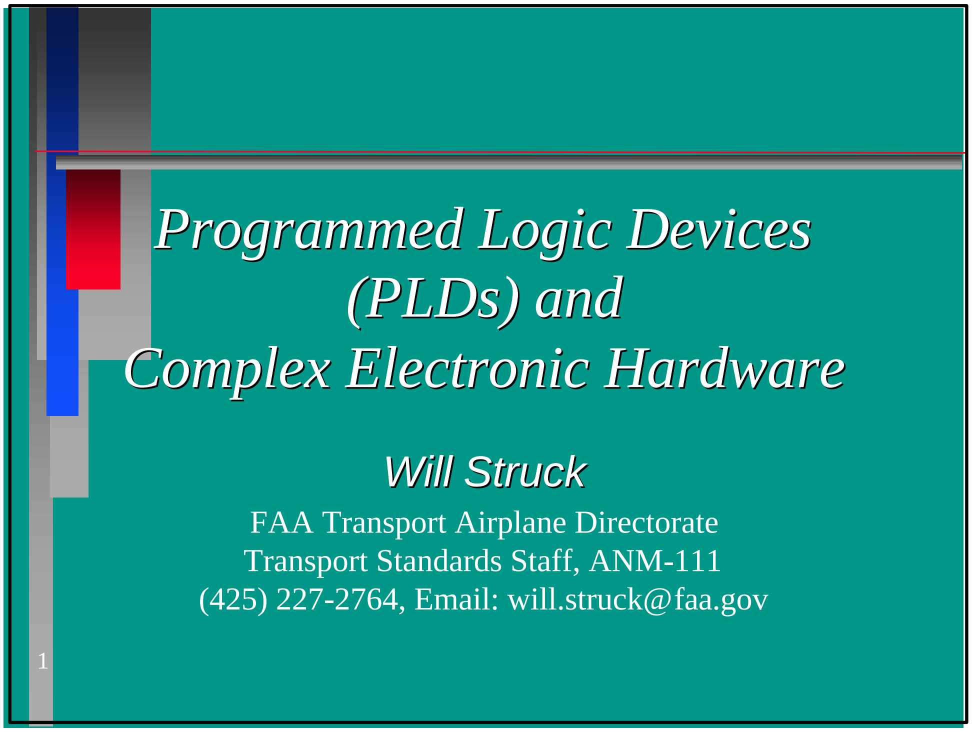
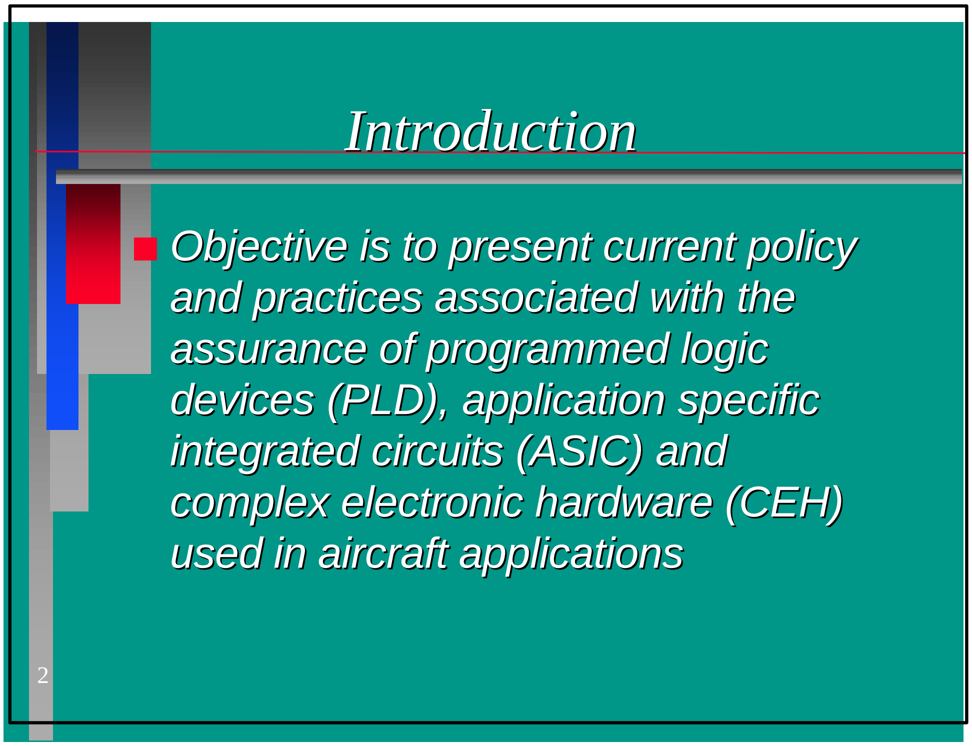


Programmed Logic Devices (PLDs) and Complex Electronic Hardware

Will Struck

FAA Transport Airplane Directorate
Transport Standards Staff, ANM-111
(425) 227-2764, Email: will.struck@faa.gov

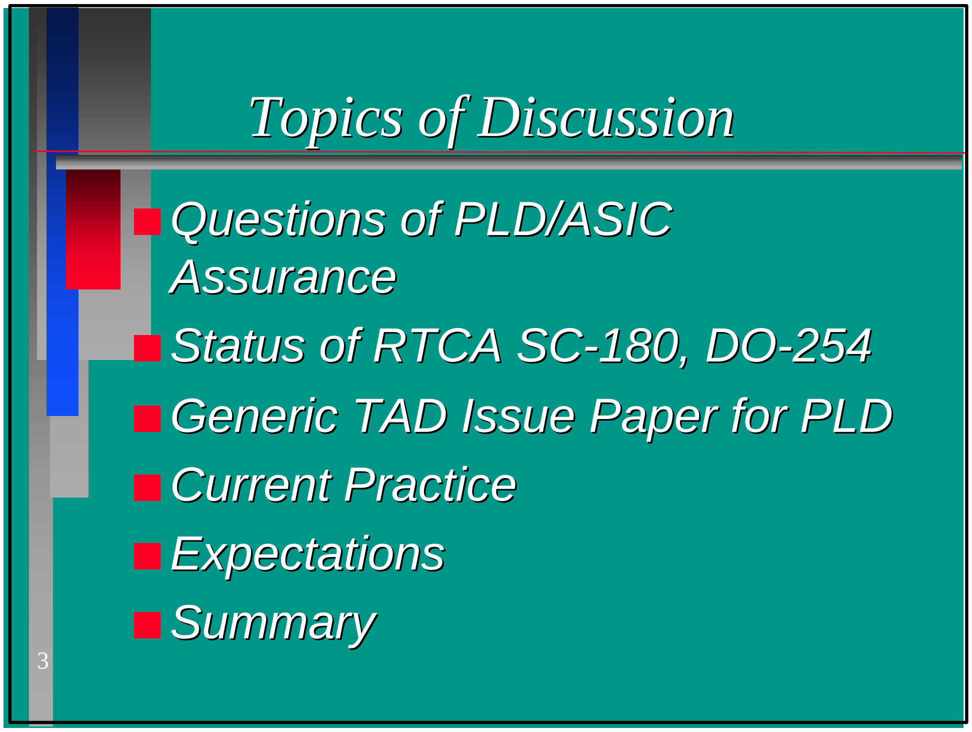
1



Introduction

- *Objective is to present current policy and practices associated with the assurance of programmed logic devices (PLD), application specific integrated circuits (ASIC) and complex electronic hardware (CEH) used in aircraft applications*

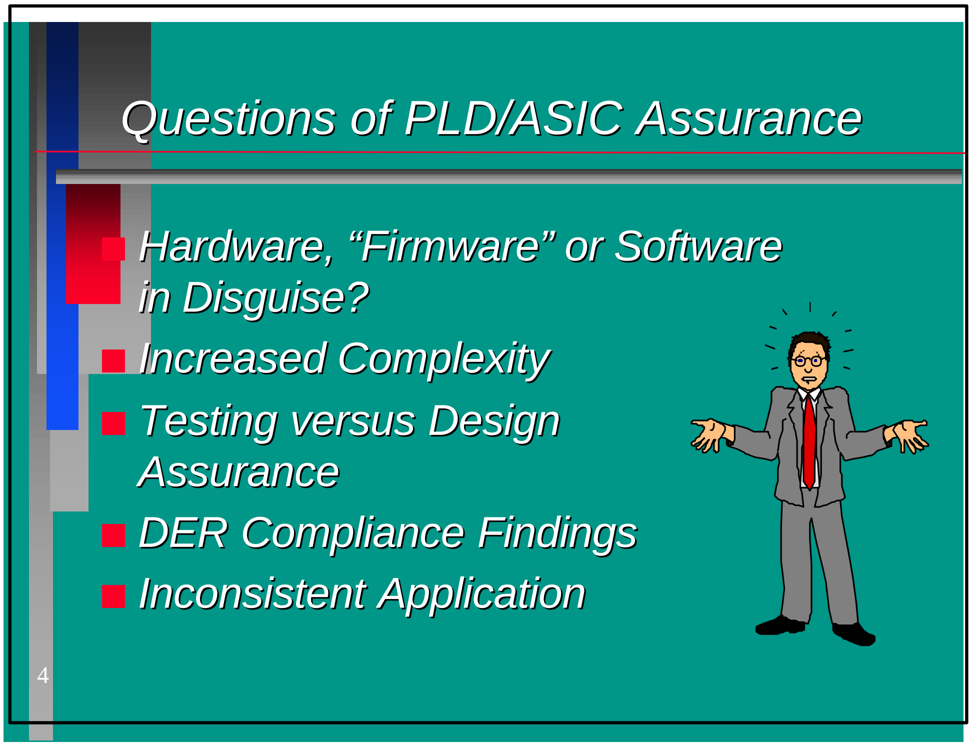
2



Topics of Discussion

- Questions of PLD/ASIC Assurance
- Status of RTCA SC-180, DO-254
- Generic TAD Issue Paper for PLD
- Current Practice
- Expectations
- Summary

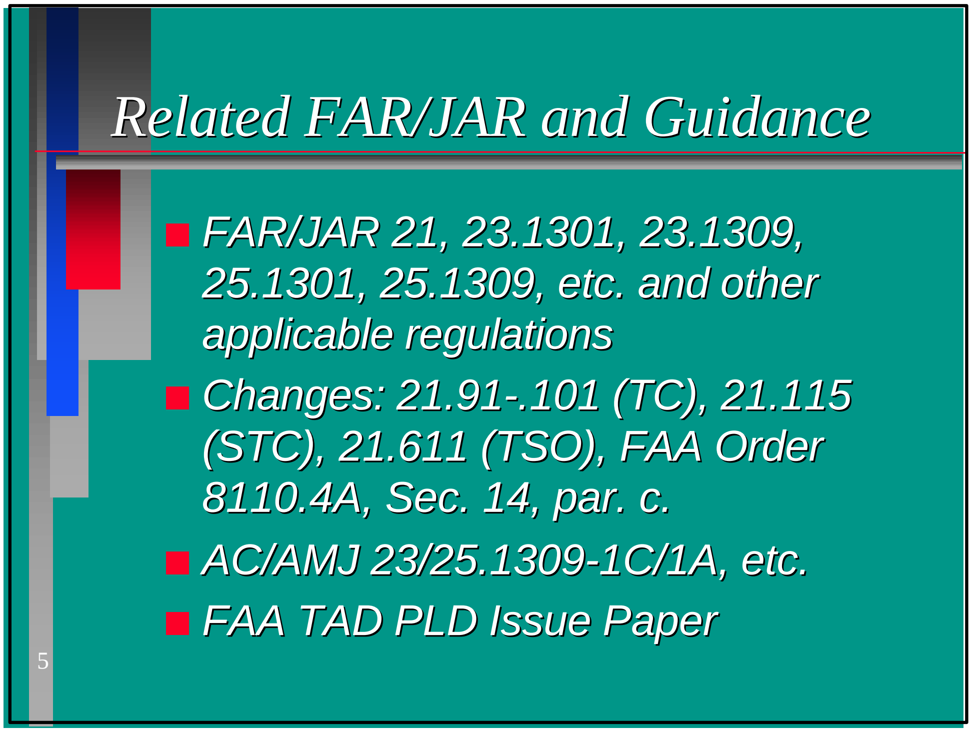
3



Questions of PLD/ASIC Assurance

- Hardware, “Firmware” or Software in Disguise?
- Increased Complexity
- Testing versus Design Assurance
- DER Compliance Findings
- Inconsistent Application

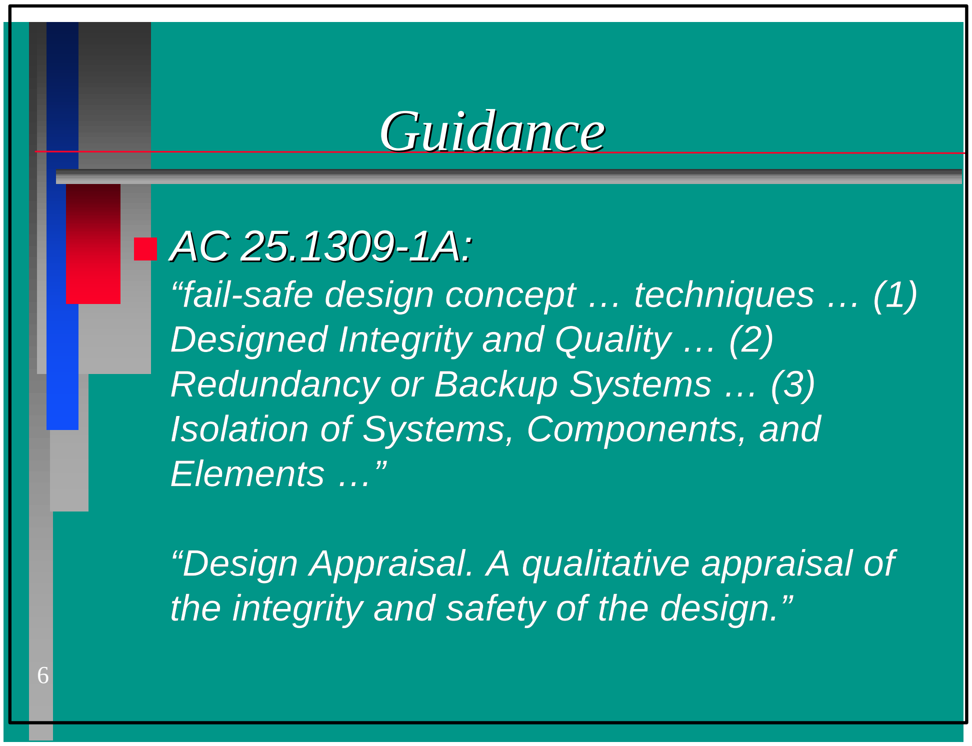
4



Related FAR/JAR and Guidance

- FAR/JAR 21, 23.1301, 23.1309, 25.1301, 25.1309, etc. and other applicable regulations
- Changes: 21.91-.101 (TC), 21.115 (STC), 21.611 (TSO), FAA Order 8110.4A, Sec. 14, par. c.
- AC/AMJ 23/25.1309-1C/1A, etc.
- FAA TAD PLD Issue Paper

5

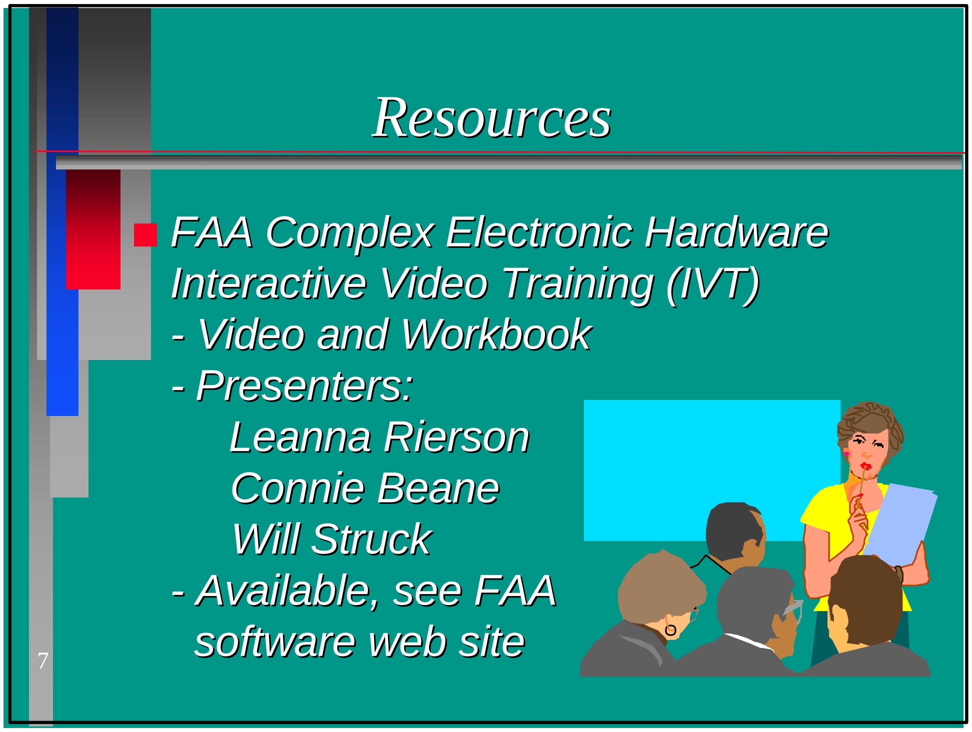


Guidance

- AC 25.1309-1A:
  “fail-safe design concept … techniques … (1) Designed Integrity and Quality … (2) Redundancy or Backup Systems … (3) Isolation of Systems, Components, and Elements …”

  “Design Appraisal. A qualitative appraisal of the integrity and safety of the design.”

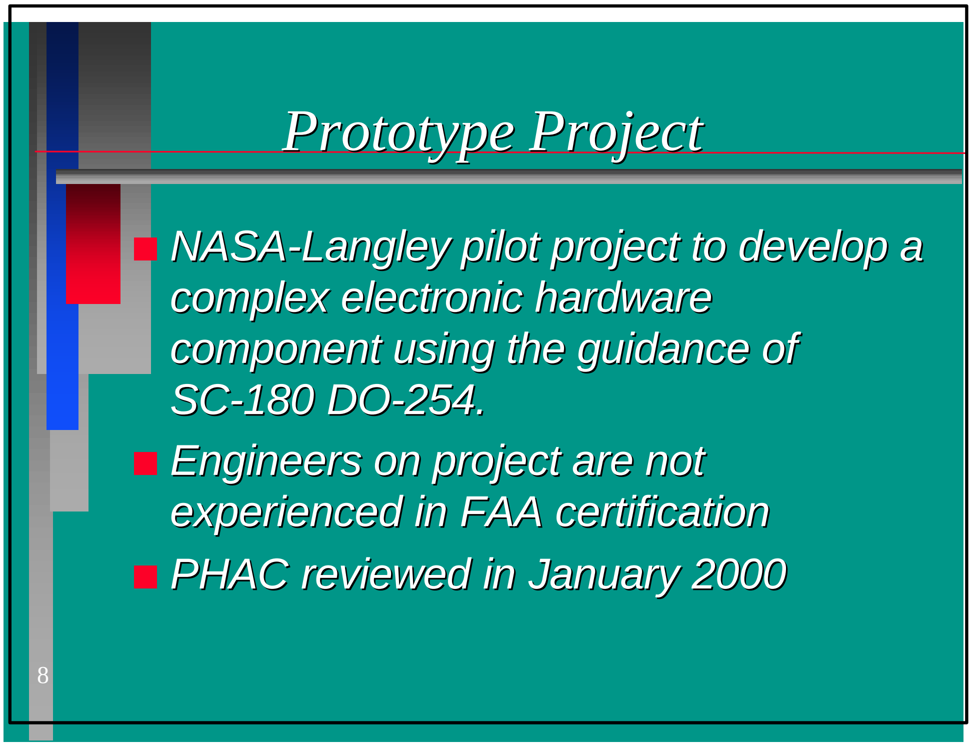
6



Resources

- FAA Complex Electronic Hardware Interactive Video Training (IVT)
  - Video and Workbook
  - Presenters:
    Leanna Rierson
    Connie Beane
    Will Struck
  - Available, see FAA software web site

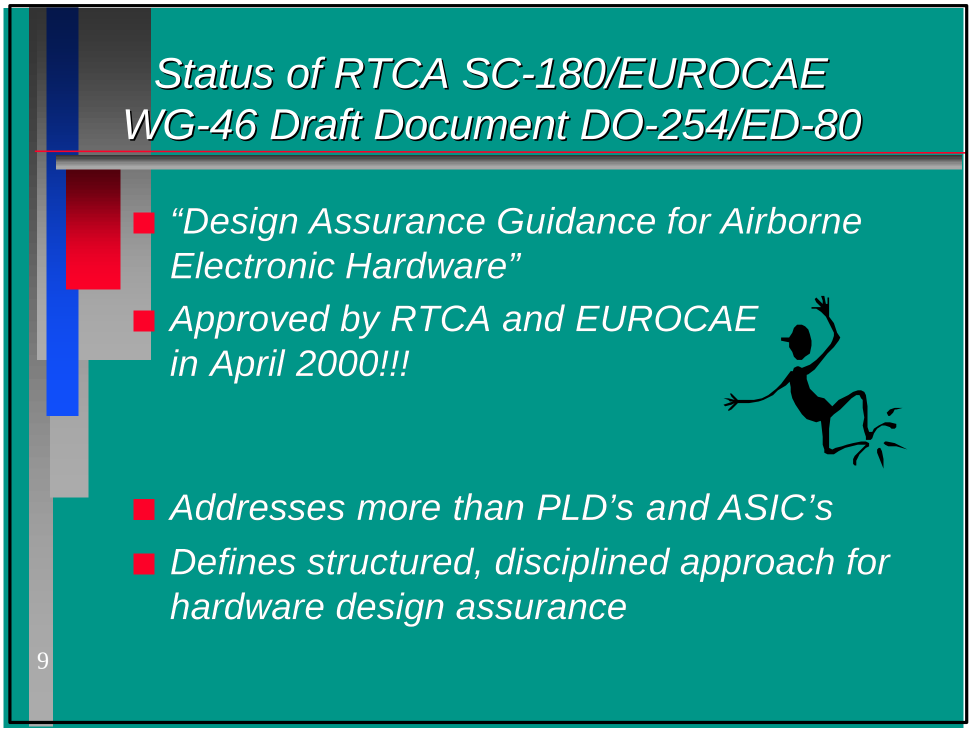
7



Prototype Project

- NASA-Langley pilot project to develop a complex electronic hardware component using the guidance of SC-180 DO-254.
- Engineers on project are not experienced in FAA certification
- PHAC reviewed in January 2000

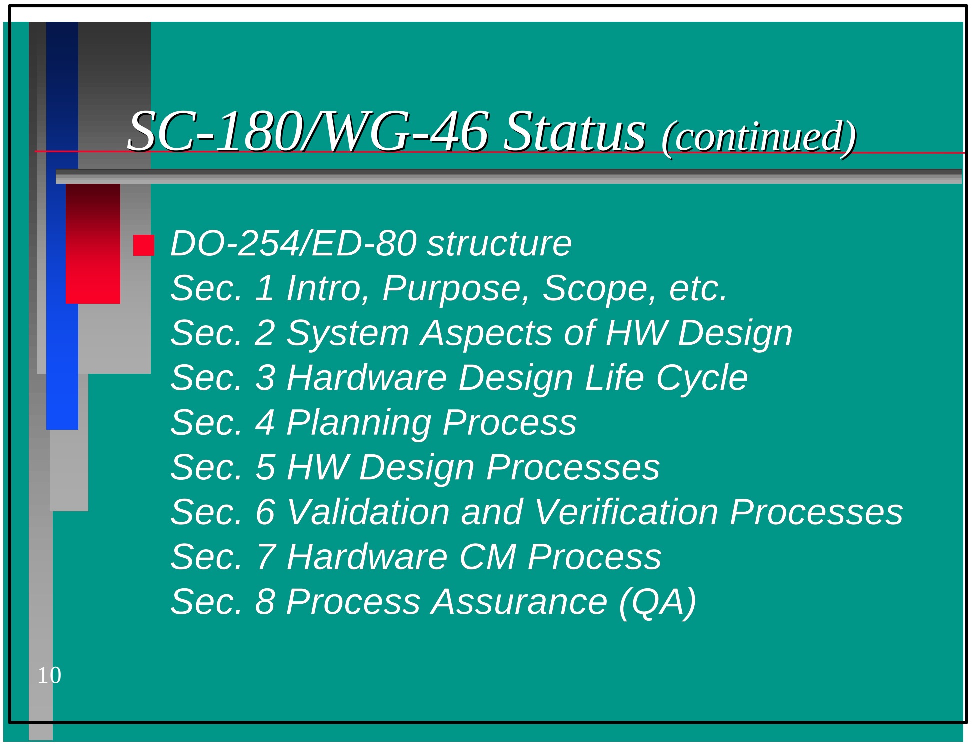
8



Status of RTCA SC-180/EUROCAE WG-46 Draft Document DO-254/ED-80

- "Design Assurance Guidance for Airborne Electronic Hardware"
- Approved by RTCA and EUROCAE in April 2000!!!
- Addresses more than PLD's and ASIC's
- Defines structured, disciplined approach for hardware design assurance

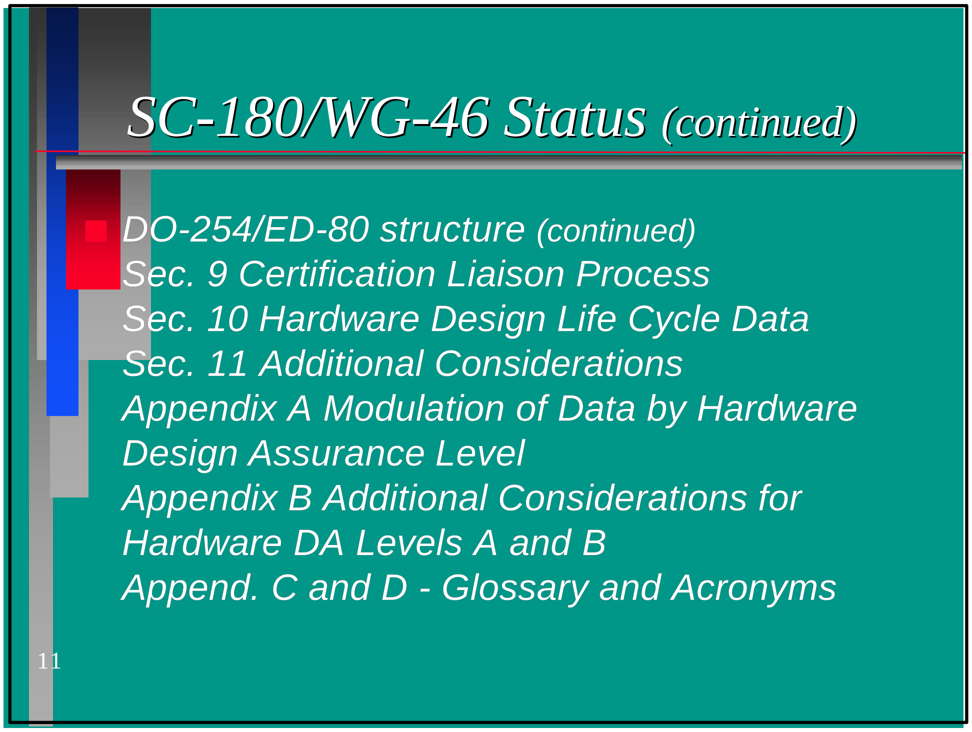
9



SC-180/WG-46 Status (continued)

- DO-254/ED-80 structure
  Sec. 1 Intro, Purpose, Scope, etc.
  Sec. 2 System Aspects of HW Design
  Sec. 3 Hardware Design Life Cycle
  Sec. 4 Planning Process
  Sec. 5 HW Design Processes
  Sec. 6 Validation and Verification Processes
  Sec. 7 Hardware CM Process
  Sec. 8 Process Assurance (QA)

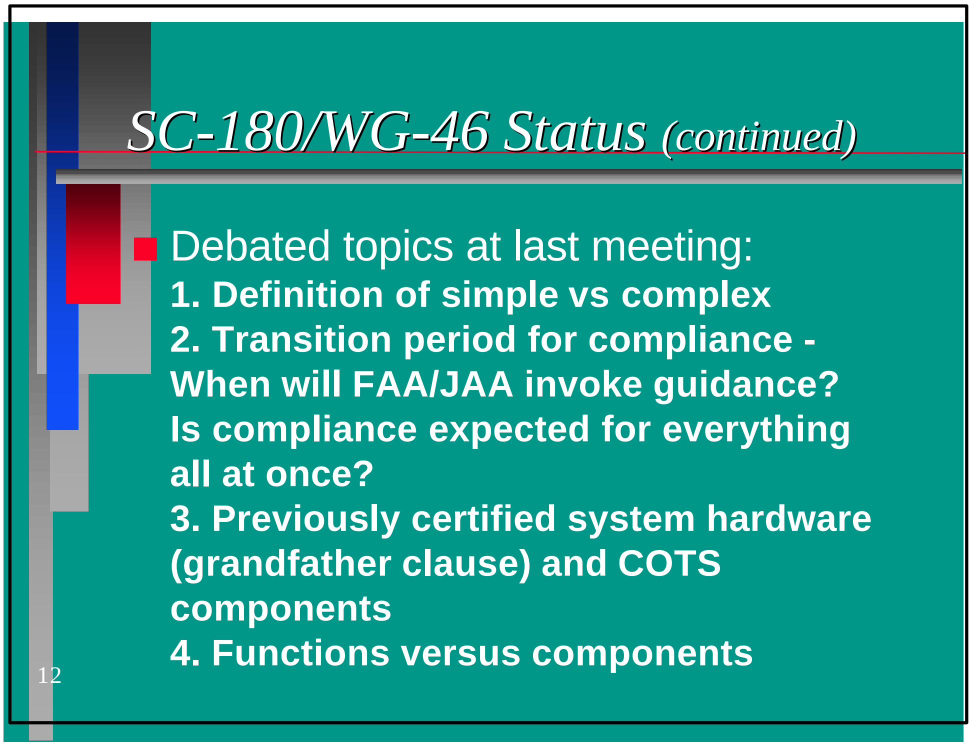
10



SC-180/WG-46 Status (continued)

- *DO-254/ED-80 structure (continued)*
  Sec. 9 Certification Liaison Process
  Sec. 10 Hardware Design Life Cycle Data
  Sec. 11 Additional Considerations
  Appendix A Modulation of Data by Hardware Design Assurance Level
  Appendix B Additional Considerations for Hardware DA Levels A and B
  Append. C and D - Glossary and Acronyms

11

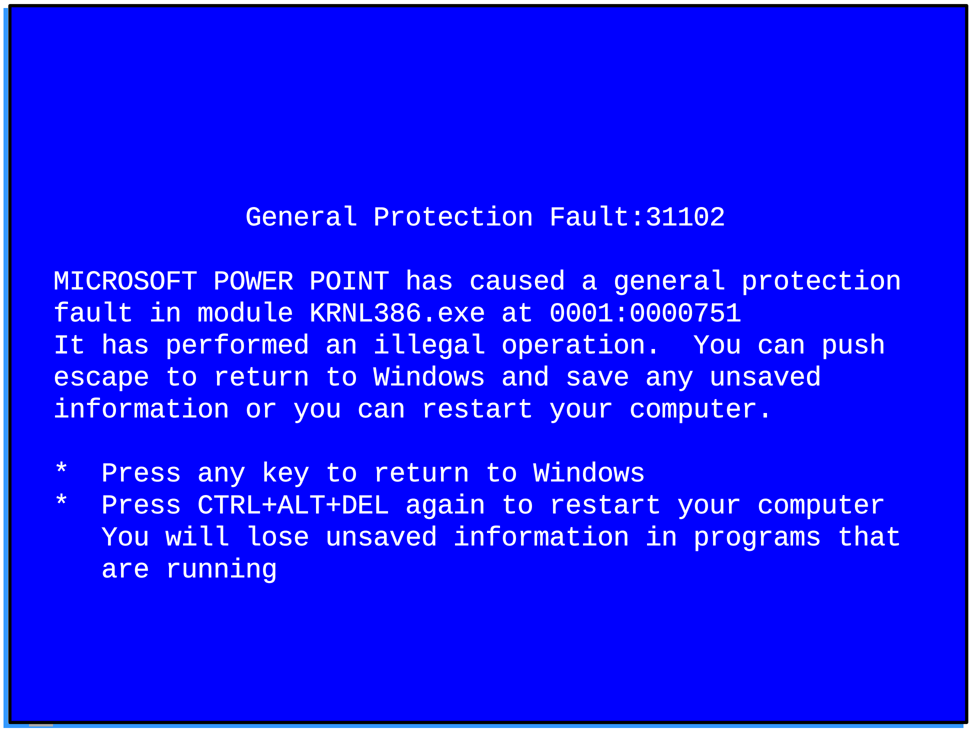


SC-180/WG-46 Status (continued)

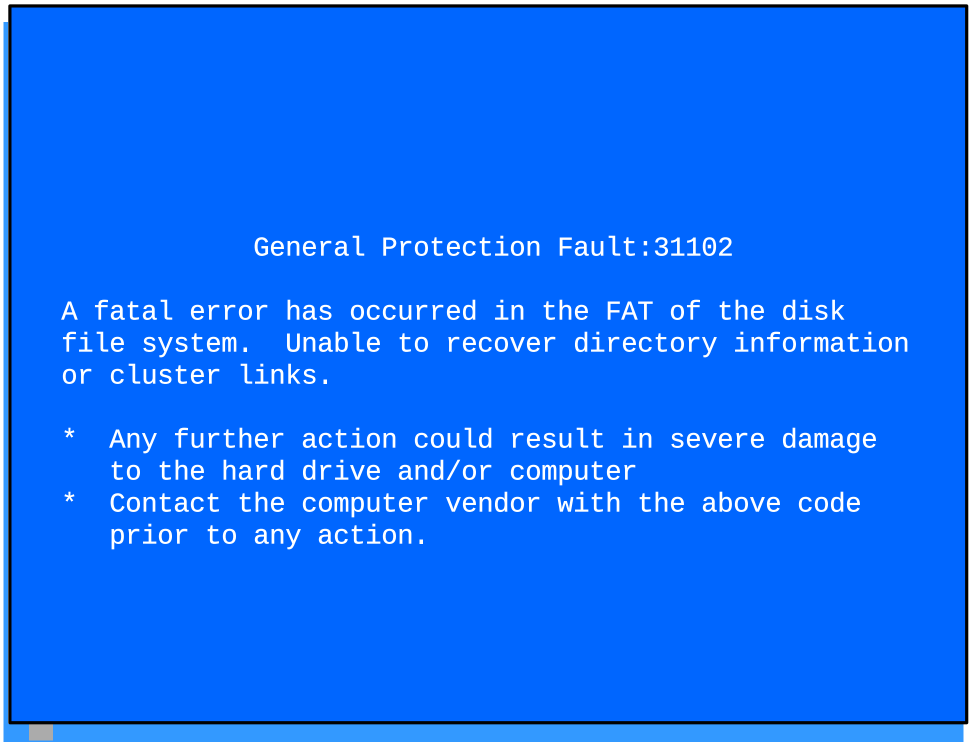
- Debated topics at last meeting:
  1. Definition of simple vs complex
  2. Transition period for compliance - When will FAA/JAA invoke guidance? Is compliance expected for everything all at once?
  3. Previously certified system hardware (grandfather clause) and COTS components
  4. Functions versus components

12

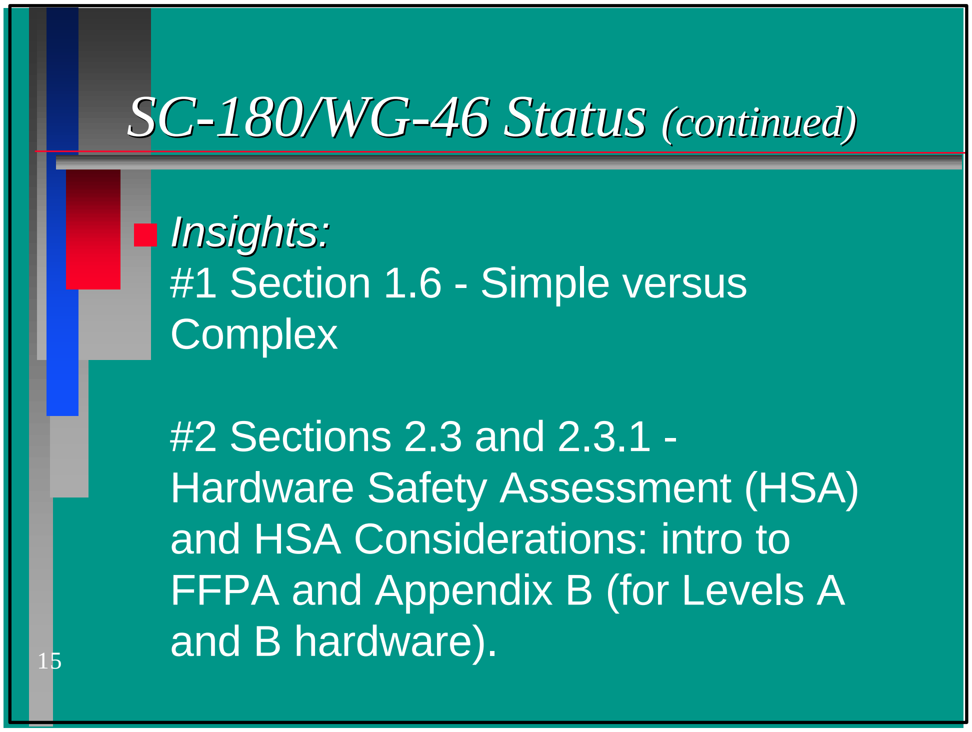
FAA National Software Conference
Complex Electronic Hardware



```
                General Protection Fault:31102

MICROSOFT POWER POINT has caused a general protection
fault in module KRNL386.exe at 0001:0000751
It has performed an illegal operation.  You can push
escape to return to Windows and save any unsaved
information or you can restart your computer.

*   Press any key to return to Windows
*   Press CTRL+ALT+DEL again to restart your computer
    You will lose unsaved information in programs that
    are running
```



```
                General Protection Fault:31102

A fatal error has occurred in the FAT of the disk
file system.  Unable to recover directory information
or cluster links.

*   Any further action could result in severe damage
    to the hard drive and/or computer
*   Contact the computer vendor with the above code
    prior to any action.
```

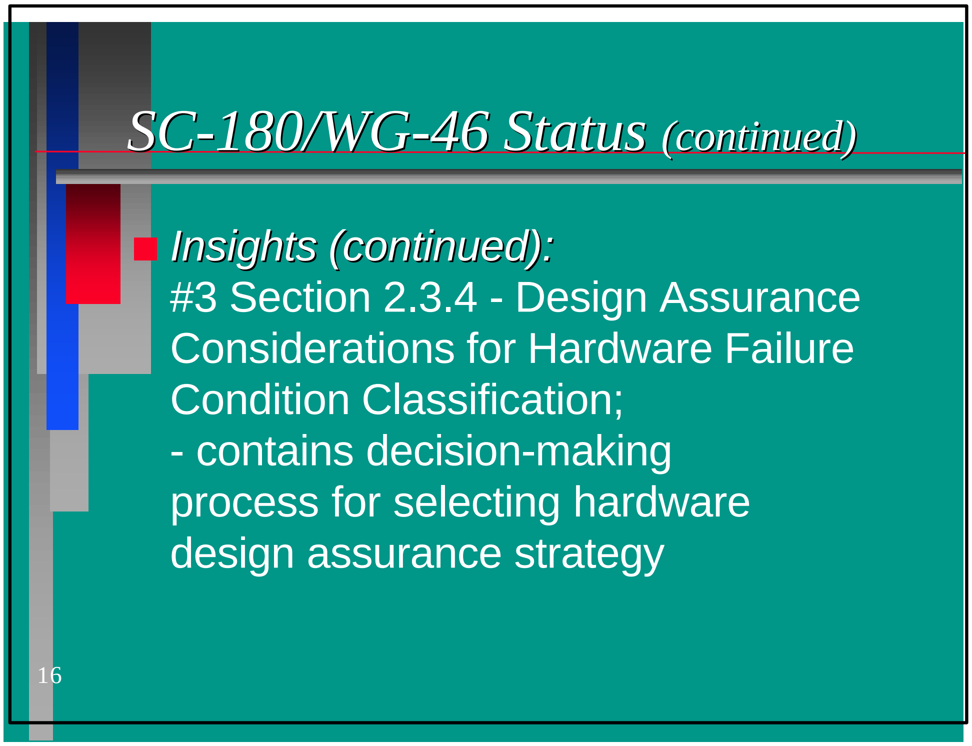


SC-180/WG-46 Status (continued)

- *Insights:*
  #1 Section 1.6 - Simple versus Complex

  #2 Sections 2.3 and 2.3.1 - Hardware Safety Assessment (HSA) and HSA Considerations: intro to FFPA and Appendix B (for Levels A and B hardware).

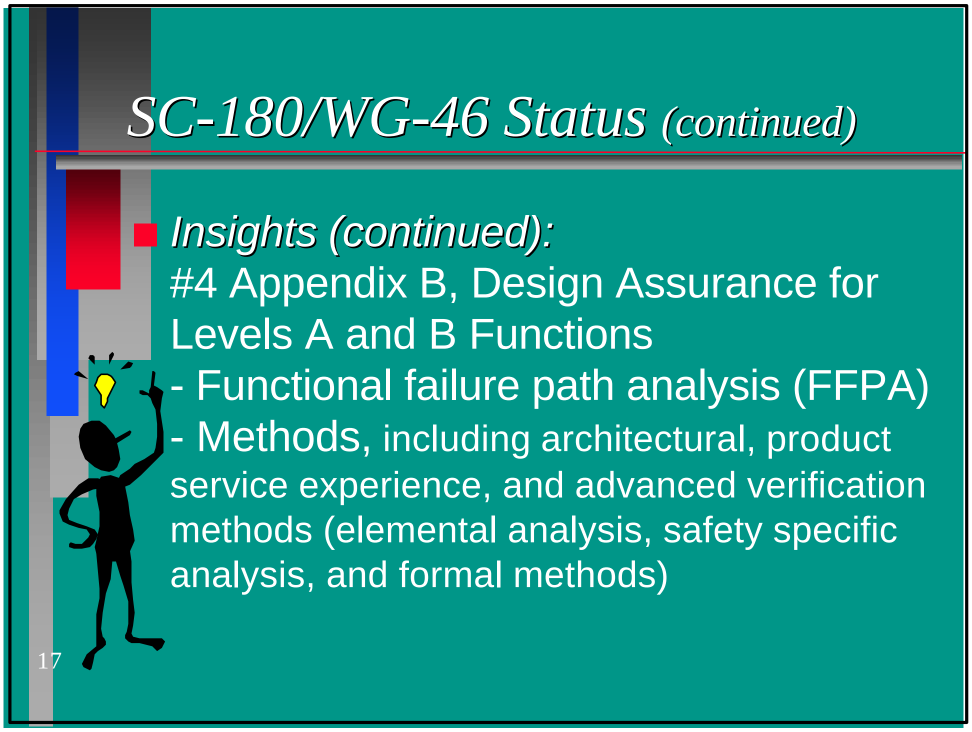
15



SC-180/WG-46 Status (continued)

- *Insights (continued):*
  #3 Section 2.3.4 - Design Assurance Considerations for Hardware Failure Condition Classification;
  - contains decision-making process for selecting hardware design assurance strategy

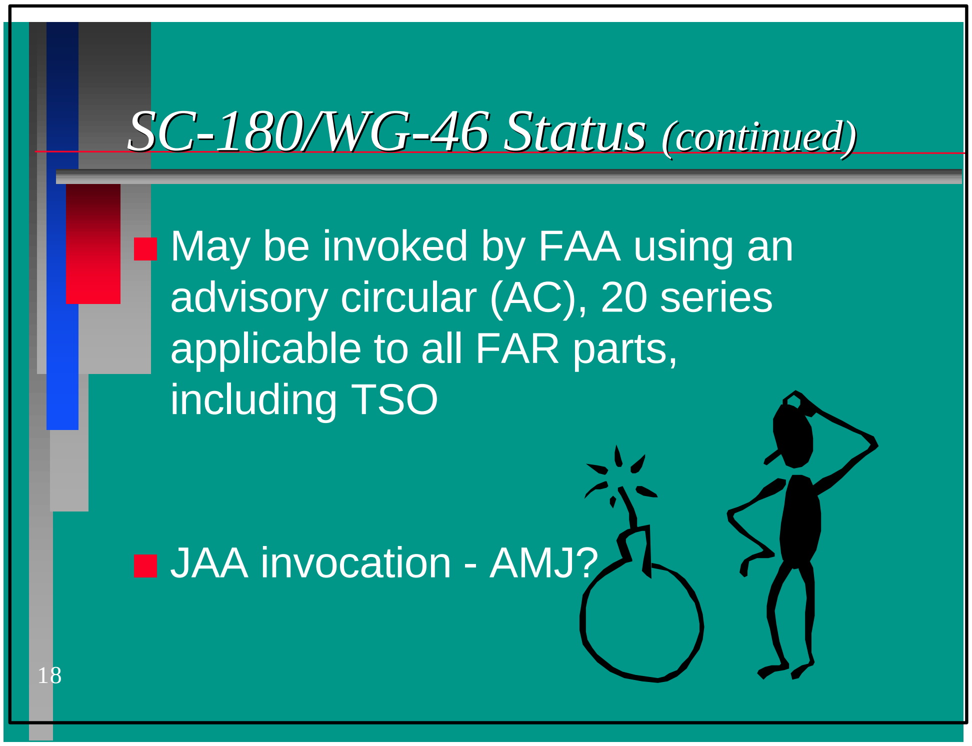
16



SC-180/WG-46 Status *(continued)*

- *Insights (continued):*
  #4 Appendix B, Design Assurance for Levels A and B Functions
  - Functional failure path analysis (FFPA)
  - Methods, including architectural, product service experience, and advanced verification methods (elemental analysis, safety specific analysis, and formal methods)

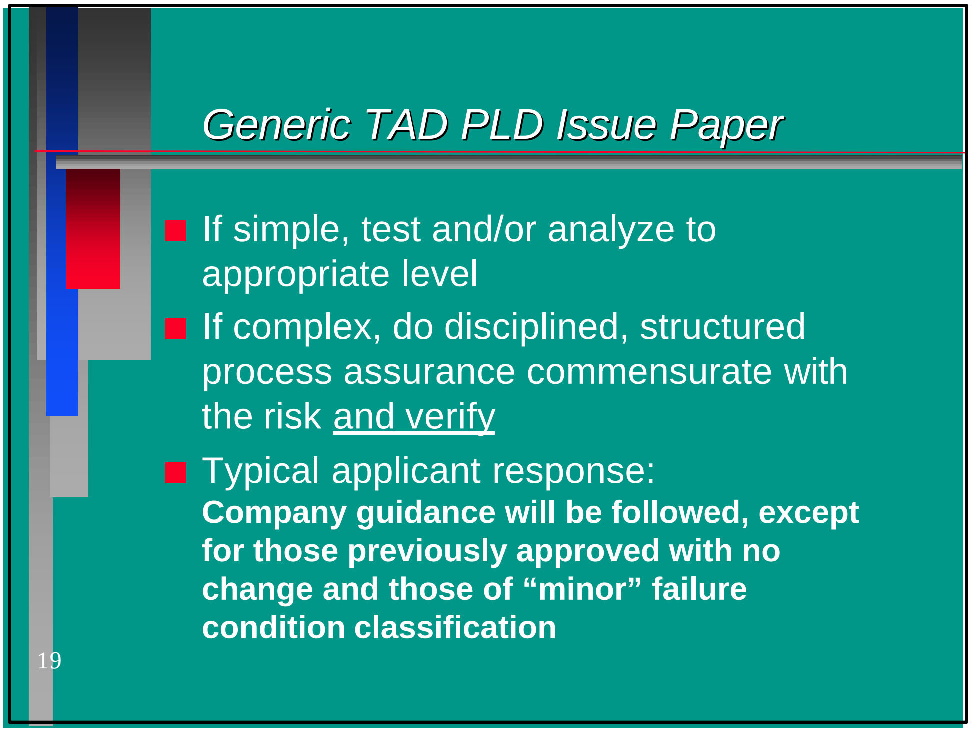
17



SC-180/WG-46 Status *(continued)*

- May be invoked by FAA using an advisory circular (AC), 20 series applicable to all FAR parts, including TSO
- JAA invocation - AMJ?

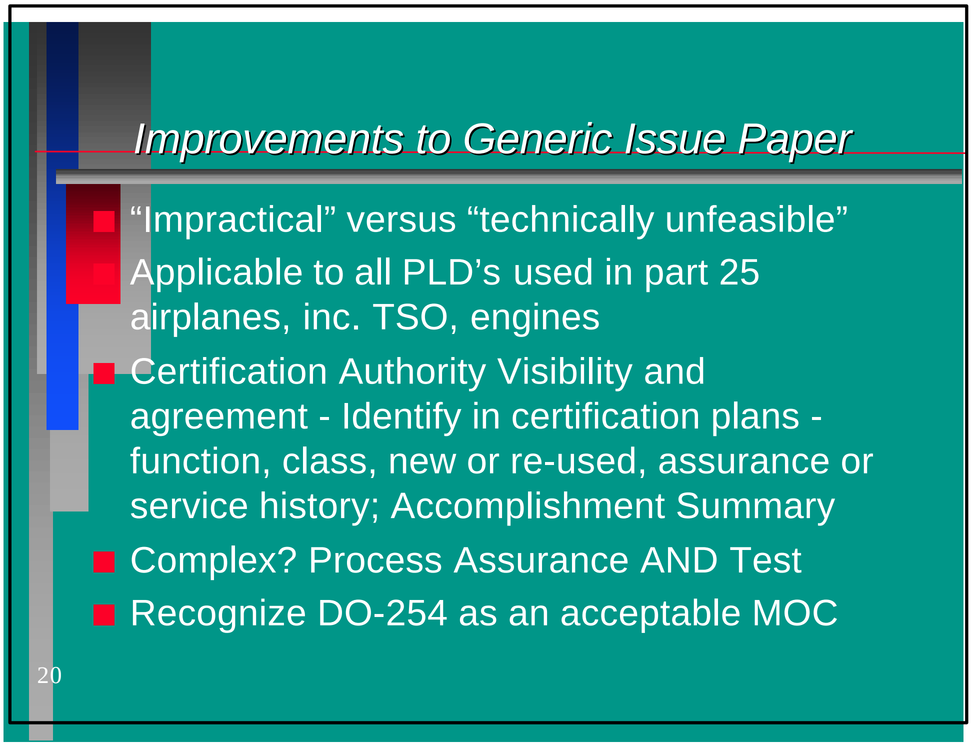
18



Generic TAD PLD Issue Paper

- If simple, test and/or analyze to appropriate level
- If complex, do disciplined, structured process assurance commensurate with the risk and verify
- Typical applicant response: **Company guidance will be followed, except for those previously approved with no change and those of “minor” failure condition classification**

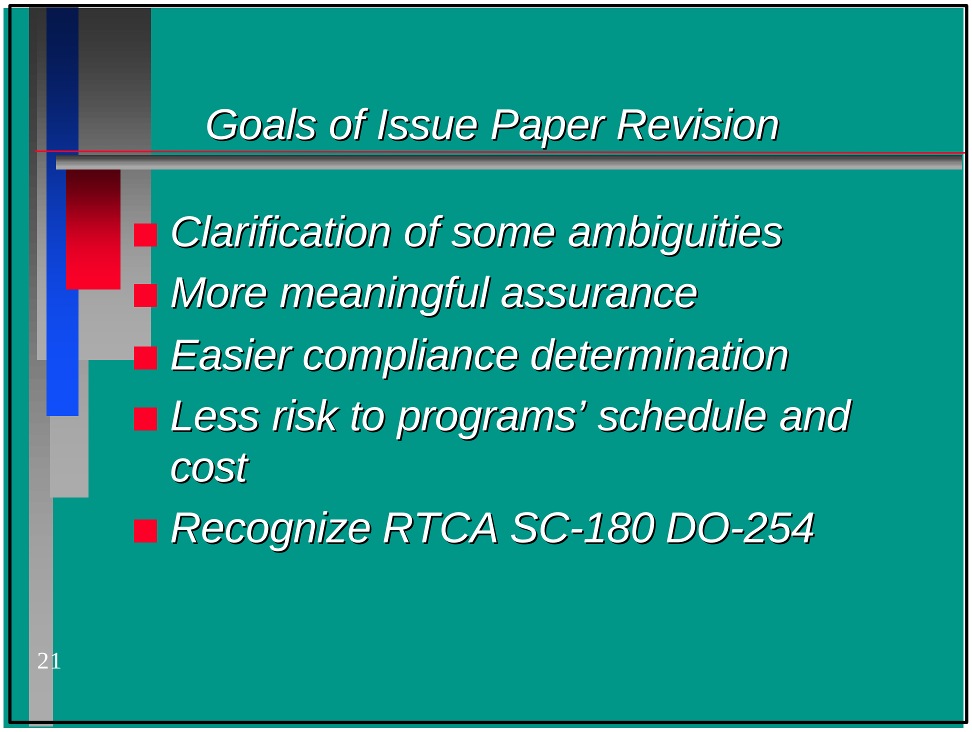
19



Improvements to Generic Issue Paper

- “Impractical” versus “technically unfeasible”
- Applicable to all PLD’s used in part 25 airplanes, inc. TSO, engines
- Certification Authority Visibility and agreement - Identify in certification plans - function, class, new or re-used, assurance or service history; Accomplishment Summary
- Complex? Process Assurance AND Test
- Recognize DO-254 as an acceptable MOC

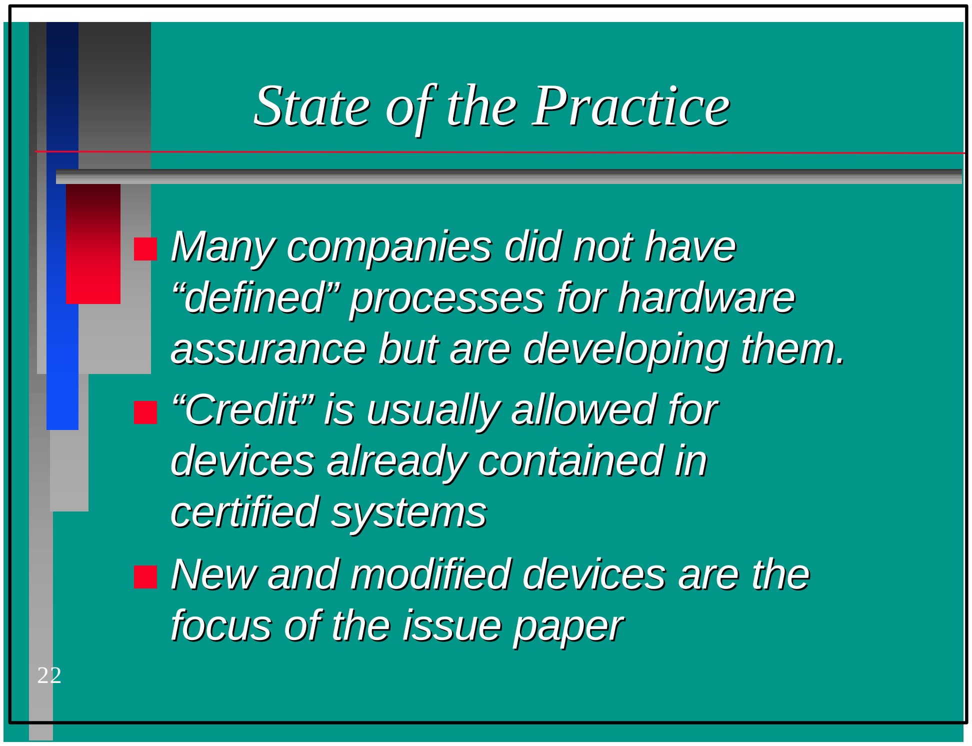
20



Goals of Issue Paper Revision

- Clarification of some ambiguities
- More meaningful assurance
- Easier compliance determination
- Less risk to programs' schedule and cost
- Recognize RTCA SC-180 DO-254

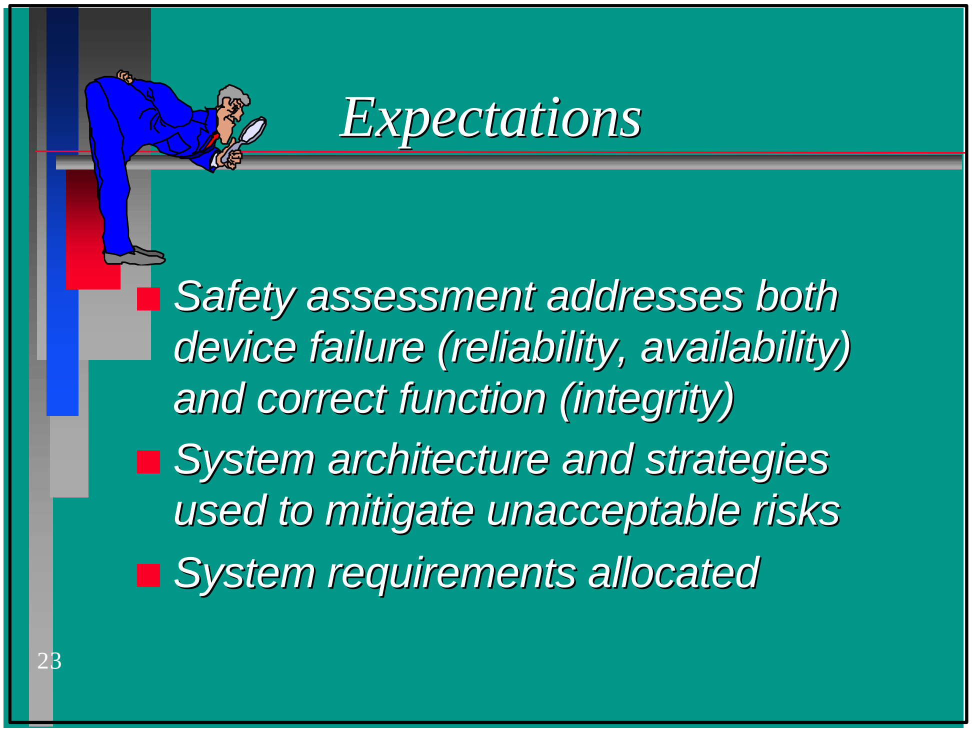
21



State of the Practice

- Many companies did not have "defined" processes for hardware assurance but are developing them.
- "Credit" is usually allowed for devices already contained in certified systems
- New and modified devices are the focus of the issue paper

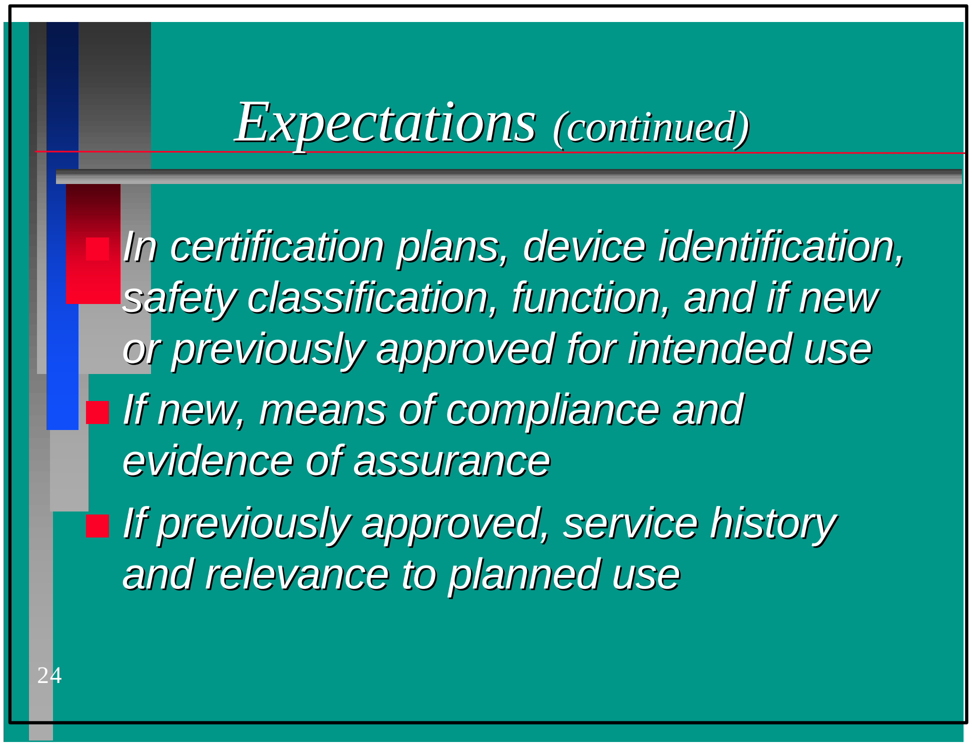
22



Expectations

- *Safety assessment addresses both device failure (reliability, availability) and correct function (integrity)*
- *System architecture and strategies used to mitigate unacceptable risks*
- *System requirements allocated*

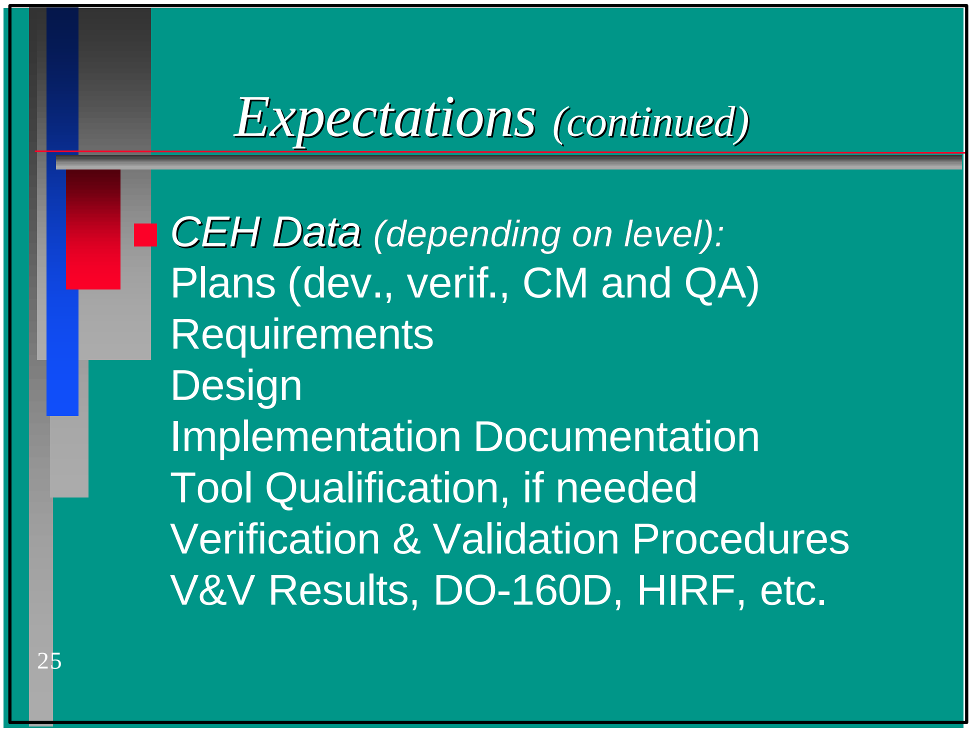
23



Expectations (continued)

- *In certification plans, device identification, safety classification, function, and if new or previously approved for intended use*
- *If new, means of compliance and evidence of assurance*
- *If previously approved, service history and relevance to planned use*

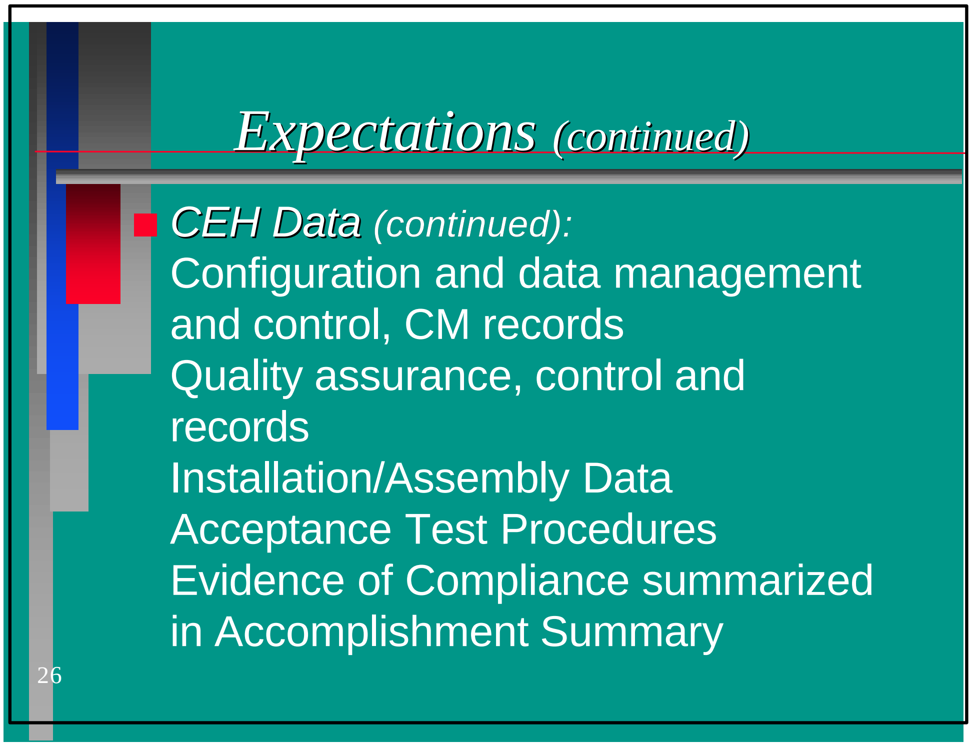
24



Expectations *(continued)*

- *CEH Data (depending on level):*
  Plans (dev., verif., CM and QA)
  Requirements
  Design
  Implementation Documentation
  Tool Qualification, if needed
  Verification & Validation Procedures
  V&V Results, DO-160D, HIRF, etc.

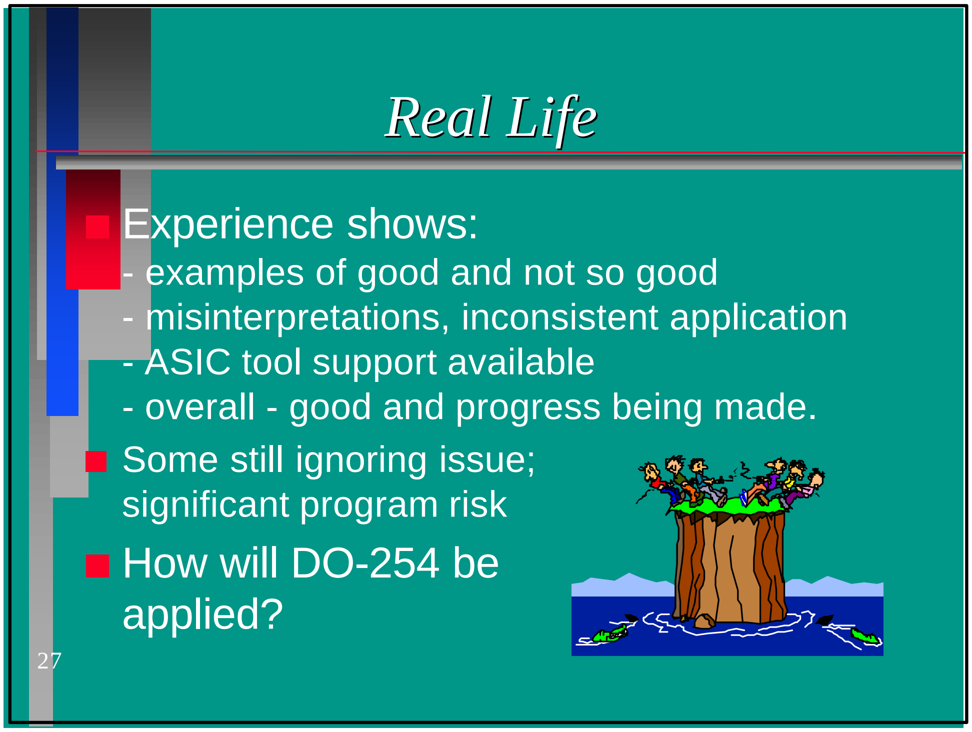
25



Expectations *(continued)*

- *CEH Data (continued):*
  Configuration and data management and control, CM records
  Quality assurance, control and records
  Installation/Assembly Data
  Acceptance Test Procedures
  Evidence of Compliance summarized in Accomplishment Summary

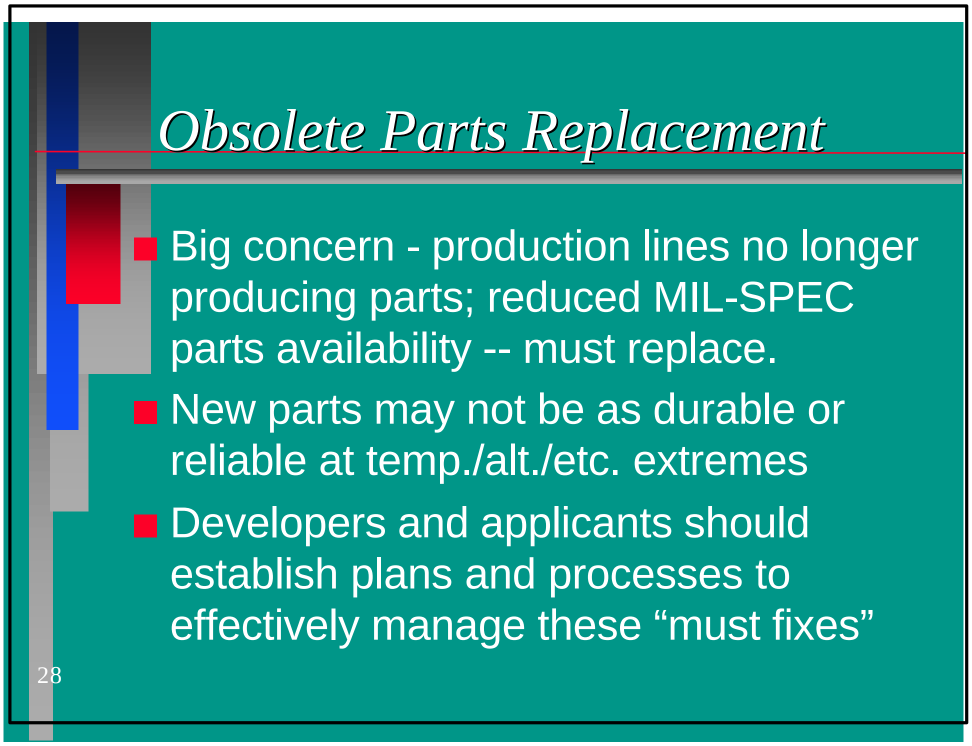
26



Real Life

- Experience shows:
  - examples of good and not so good
  - misinterpretations, inconsistent application
  - ASIC tool support available
  - overall - good and progress being made.
- Some still ignoring issue; significant program risk
- How will DO-254 be applied?

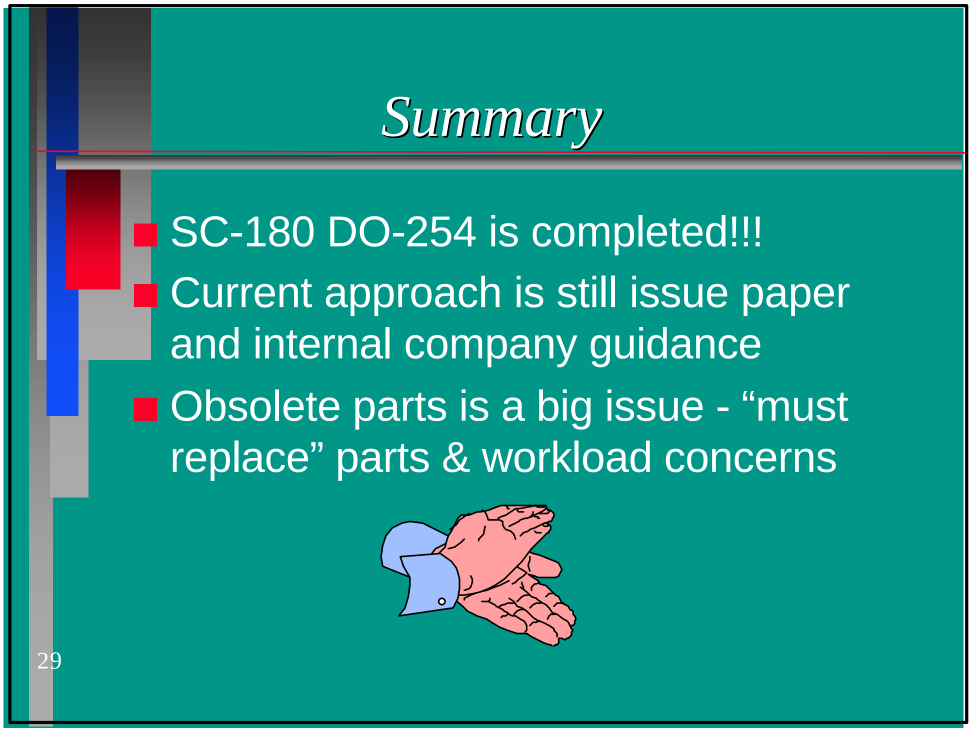
27



Obsolete Parts Replacement

- Big concern - production lines no longer producing parts; reduced MIL-SPEC parts availability -- must replace.
- New parts may not be as durable or reliable at temp./alt./etc. extremes
- Developers and applicants should establish plans and processes to effectively manage these “must fixes”

28



Summary

- SC-180 DO-254 is completed!!!
- Current approach is still issue paper and internal company guidance
- Obsolete parts is a big issue - “must replace” parts & workload concerns

29